Schegge di Cassandra/ OHM2013: Access! Now!

(301))— La Rete innerva tutto il mondo, e in tutto il mondo è strumento di affrancamento, e anche di oppressione. Ma c'è chi lotta per…

Schegge di Cassandra/ OHM2013: Access! Now!

Figure 1:

(301))— La Rete innerva tutto il mondo, e in tutto il mondo è strumento di affrancamento, e anche di oppressione. Ma c'è chi lotta per garantire che la Rete sia trattata come si deve.

4 ottobre 2013—Con questa ultima "Scheggia" si chiude la serie di pillole che Cassandra ha potuto confezionare grazie ad OHM2013 ed a tutti gli amici dell'Ambasciata. In effetti, a giudicare dai pochi commenti nei forum, si direbbe che le "pillole di contenuti" non siano molto popolari nemmeno tra i 24 incontentabili lettori, e così cambiamo tema.

Si fa un grande parlare, ed a buona ragione, delle intercettazioni del Datagate (grazie Edward), ma ci si dimentica che le tecniche di intercettazione sviluppate negli ultimi 10 anni sono a disposizione delle più svariate categorie di "cattivi" e "spioni" di turno, che non vogliono controllare il mondo, ma magari si accontentano del risultato delle elezioni, o del contenuto degli articoli di qualche giornalista. Questo avviene regolarmente in paesi a democrazia "formale" o "nulla", come ce ne sono tanti al mondo (Asia ed Africa in primis, ma non solo…).

Per essere un Piccolo Grande Fratello in questi casi basta molto poco, e chi si trova a dover usare la Rete di questi paesi, magari avvicinandosi ad essa per la prima volta, può correre rischi piuttosto gravi. Il mondo è infatti pieno di individui ed ancor più di aziende disposte a vendere tecnologie e consulenze a chiunque e per qualsiasi scopo.Cosa possono fare quindi coloro che in queste condizioni si trovano?

Beh, possono rinunciare alla Rete, per esempio. Possono diventare esperti software e di sicurezza. Oppure possono fare del loro meglio e rischiare.

Oppure… Oppure possono chiedere aiuto.

Al mondo esistono parecchie persone ed organizzazioni che in una certa misura possono fornirlo come attività collaterale. Ne esiste anche una che si dedica solo a questo, AccessNow.org, che è attiva da anni ed ha fatto della garanzia di un accesso alla Rete e del rispondere alle richieste d'aiuto più svariate la propria unica missione.

Sono attivi 24 ore al giorno, 7 giorni alla settimana, lavorano su 3 sedi, (Tunisi, San José, Seul) supportano le lingue più svariate ed esotiche ed implementano processi formalizzati di gestione degli incidenti, di addestramento di volontari e di personale, e di escalation dei problemi più complessi. Volendo semplificare al massimo, si tratta di una difesa della società civile da chi vuole utilizzare la Rete contro "altri".

Di casi clamorosi di giornalisti intercettati in Italia ce ne sono stati di così famosi da non meritare nemmeno di essere ricordati.

Ma cosa dire di un partito di governo che gestisce le elezioni usando i software di "personal management", falsificando i nomi di dominio dei blog "scomodi", inondando i forum di falsi commenti di falsi utenti, proprio come succede sui siti aziendali e sui motori di ricerca di viaggi e hotel?O che usa l'intimidazione come arma dietro il paravento della pirateria o della pedopornografia?

O che semplicemente si limita a censurare l'accesso in Rete dei suoi cittadini? Bene, per contribuire ad impedire tutto questo, Access utilizza la quantità di tecnologie necessarie, comprese le più esoteriche: in casi estremi installano sui pc di chi lo richiede degli Intrusion Detection System per rivelare tentativi di trojanizzazione o di violazione del personal computer, ad esempio di un giornalista investigativo.Durante l'interessante intervento, oltre ad una descrizione dell'organizzazione, lo speaker di Access ha presentato una impressionante serie di dettagliate statistiche da loro elaborate.

Il punto centrale è elementare: in ogni paese ci sono le leggi contro tutti i tipi di criminali: non ci sarebbe perciò nessun bisogno di iniziative specifiche in Rete di lotta alla criminalità, o a particolari tipi di criminalità.

Ma chi conosce anche solo la rete di relazioni delle persone controlla le persone stesse: è per questo che le intercettazioni, legali o meno che siano, hanno perfettamente senso, specialmente da parti di entità governative.

Una per tutte: durante l'attività di gestione degli incidenti ed attacchi da loro svolta, la percentuale degli attacchi rilevati attribuiti a governi di varia legittimità è stata del 77 per cento, quelli di governi associati con "altre organizzazioni" del 17 per cento e quella di organizzazioni o individui "isolati" solo il 5 per cento.

Questo è confermato anche dal fatto che negli anni passati la maggioranza degli azioni difensive intraprese era a favore di chi si vedeva negato un accesso alla Rete, mentre oggi la maggior parte dei problemi è provocato proprio dall'accesso alla Rete per come viene regalato o fornito ad intere popolazioni.

Alla fine dell'intervento sono uscito dal tendone sentendomi un po' più confortato.

Originally published at punto-informatico.it.